PathBuildRoot

The output buffer must be large enough to hold four characters

Sean Barnum, Cigital, Inc. [vita[1]]

2007-04-02

Part "Original Cigital Coding Rule in XML"

Mime-type: text/xml, size: 3531 bytes

Attack Category	• Malicious Input • Path spoofing or confusion problem
Vulnerability Category	• Buffer Overflow • Unconditional
Software Context	• File Path Management
Location	• shlwapi.h
Description	The output buffer for the PathBuildRoot() function must be large enough to hold four characters. PathBuildRoot() creates a root path from a given drive number. The destination string buffer must be long enough to hold the return root string. The routine takes an integer (e.g. 3) and fills in a string for the root path of that drive number (e.g. "D:\"). Therefore, the buffer must receive exactly 3 characters plus a NULL character.
APIs	**Function Name** / **Comments** PathBuildRoot PathBuildRootA PathBuildRootW
Method of Attack	Attacker can cause a buffer overflow if the path variable is not at least 4 characters long.
Exception Criteria	
Solutions	**Solution Applicability** / **Solution Description** / **Solution Efficacy** Whenever PathBuildRoot or variant is used. / The output buffer, szRoot, must be at least 4 characters in length. / Effective
Signature Details	LPTSTR PathBuildRoot(

1. http://buildsecurityin.us-cert.gov/bsi/about_us/authors/35-BSI.html (Barnum, Sean)

	LPTSTR szRoot, int iDrive);

Examples of Incorrect Code	`TCHAR buffer_1[3]; // buffer is too small`
	`LPTSTR lpStr1;`
	`lpStr1 = buffer_1;`
	`cout << "The root path for 0 is " << PathBuildRoot(lpStr1,0) << endl;`

Examples of Corrected Code	`TCHAR buffer_1[4]; // buffer is correctly sized`
	`LPTSTR lpStr1;`
	`lpStr1 = buffer_1;`
	`cout << "The root path for 0 is " << PathBuildRoot(lpStr1,0) << endl;`

Source Reference	• http://msdn.microsoft.com/library/default.asp?url=/library/en-us/shellcc/platform/shell/reference/shlwapi/path/pathbuildroot.asp[2]
Recommended Resource	
Discriminant Set	**Operating System**: • Windows **Languages**: • C • C++

Cigital, Inc. Copyright

The Build Security In (BSI) portal is sponsored by the U.S. Department of Homeland Security (DHS), National Cyber Security Division. The Software Engineering Institute (SEI) develops and operates BSI. DHS funding supports the publishing of all site content.

1. mailto:copyright@cigital.com